GRC Maturity Capstone Project

Norman Shatto

A. The Proposed Project

Sandia Valley Bank (SVB) is a medium-sized bank located in Albuquerque, New Mexico, and is facing an increase in cybersecurity threats, regulatory pressures, and operational complexity as it expands its digital services to its customers. The bank is also facing increased financial, compliance, and reputational risks.

The IT business problem being investigated is that Sandia Valley Bank lacks an enterprise-wide, mature Governance, Risk, and Compliance (GRC) program that supports today's advanced cybersecurity oversight, vendor management, and regulatory compliance. To address this challenge, the proposed project will implement an enterprise-wide GRC maturity upgrade, utilizing the NIST Cybersecurity Framework, FFIEC Cybersecurity Assessment Tools, and GLBA Safeguard Rules as the governing standards for this project. The solution will include the development of a new governance structure, the creation of updated policy documents, the development of a comprehensive risk register, the mapping of existing security controls for regulatory requirements, and a multi-year roadmap for achieving enterprise-wide maturity.

This initiative is just one of several concurrent projects within the IT department at SVB. As such, the project will utilize a phased approach to balance resource allocations among departments and minimize the impact on ongoing operations. The IT department will prioritize the highest risk areas first and coordinate project timelines with the compliance, cybersecurity, and operations departments. There are multiple stakeholders involved in this project, including executive leadership, who require better oversight, compliance teams that need audit-ready documentation, IT and security staff who require clear processes, and vendors whose risk level must be continually evaluated.

Key implementation aspects of this project include governance design, maturity assessment, remediation planning for control gaps, enhanced vendor risk management, and the development of security metrics. The success of this project will be measured against specific Key Performance Indicators (KPIs), including improvements in maturity scores, reductions in high-risk findings, compliance rates of policies, vendor risk ratings, and increased transparency into the bank's cybersecurity posture.

B. Project Design and Implementation Phase

The lack of a formally structured GRC process at SVB creates an increasingly large gap between the increasing volume of cybersecurity and compliance risks. While there are no IT security policies, risk assessments, or vendor oversight practices, these are being performed in a disorganized manner, resulting in inconsistent control application and limited visibility into overall organizational risks. The root cause of this issue is largely due to Sandia Valley Bank's rapid growth through digital means, the use of third-party vendors, outdated documentation, and the lack of a common method of identifying and mitigating cyber threats. Regulatory expectations continue to rise, while malicious actors remain aggressive in targeting financial institutions with cyberattacks. The current model of SVB will not provide the necessary oversight to support a modern banking environment.

Executive leadership lacks reliable reporting and risk analysis to make informed decisions, which leaves the organization exposed to financial and reputational loss. Compliance and audit teams have difficulty demonstrating regulatory alignment, resulting in higher levels of audit findings, which could result in Gramm-Leach-Bliley Act Safeguards Rule (GLBA) or FFIEC deficiencies.

IT and security staff lack standardized procedures to manage vulnerabilities, respond to incident scenarios, or apply consistent controls. Vendor management personnel lack the ability to accurately assess third-party risk, thereby increasing the likelihood of experiencing a supply chain-based cyberattack. Customers ultimately face an increased risk of a data breach or service disruption, which can erode their trust and long-term loyalty to the institution.

Sandia Valley Banks' GRC solution is aligned with all recognized industry standard frameworks and regulatory requirements applicable to financial institutions. Integrating the NIST cybersecurity framework enables SVB to follow a structured framework to identify, protect, detect, respond to, and recover from cybersecurity threats or vulnerabilities as recommended by NIST to enhance the security of critical infrastructure (NIST, 2018). Using the FFIEC cybersecurity assessment tool will provide a methodical approach for SVB to assess its inherent risk and maturity level for each domain, including, but not limited to, threat intelligence, incident response, and external dependency management (FFIEC, 2025).

Additionally, Sandia Valley Banks' GRC solution provides support for compliance with the GLBA, which requires administrative, technical, and physical controls to protect customer information and requires ongoing risk assessment and monitoring (Federal Trade Commission, 2024). Enhancements to policies and controls for Sandia Valley Banks' GRC solution will provide an additional layer of alignment with the Payment Card Industry Data Security Standard (PCI-DSS), which is a mandatory security standard for protecting cardholder data throughout the payment system (PCI Security Standards Council, 2024).

Aligning Sandia Valley Bank's GRC solution with these well-established standards will ensure that SVB enhances its security position, closes potential compliance gaps, and remains in regulatory compliance within a rapidly changing threat environment.

C. Cost Analysis

The estimated costs represent a typical level of investment for a banking organization to implement a modern GRC program. The largest portion of these costs will be associated with the central GRC management platform, due to its ability to enable automated risk assessments, compliant reporting, and to securely store and manage documentation within a single centralized location. Centralized GRC platforms enable a significant reduction in manual efforts and provide accurate and consistent risk data, which is crucial when operating in an extremely regulated industry such as banking.

As for labor and consulting costs, they are necessary because this project will require specific and specialized knowledge in cybersecurity, compliance, and financial industry regulations. Additionally, implementing GRC processes, creating policies, establishing a risk register, and mapping controls to regulatory frameworks all require significant collaboration among IT, security, compliance, and audit teams. These external consultants can assist in accelerating the development process, align with best practices, and provide technical assistance regarding tool configurations and integrations.

Additionally, training is a required component of the project to ensure that employees use the new GRC platform effectively. If there is no employee training on the new GRC platform, the bank runs the risk of not using the full potential of the system or failing to consistently apply risk and compliance processes throughout the organization.

The hardware and software costs associated with this project are related to ensuring secure working environments and providing employees with reliable tools to develop policies, produce reports, and perform analyses. Compared to the overall operational and regulatory benefits of improving their security posture, reducing audit findings, and strengthening organizational governance, these costs are relatively low. Overall, the cost structure of the proposed project is reasonable, given the scope of a mid-sized bank looking to modernize its GRC operations and enhance its cybersecurity resiliency.

Cost Category	Description	Estimated Cost
Hardware	Buy workstation upgrades for GRC analysts	$3,600
Software Tools	GRC management platform	$45,000 annually
Licensing	SIEM log and compliance reporting modules	$12,000
Consulting and Labor	External cybersecurity consultant support	$24,000
Internal Labor	IT, compliance, and security employees for design and development	$26,000
Training and Implementation	Vendor training for GRC platform	$9,000
Miscellaneous	Documentation tools, secure file storage, and analyst reference materials	$1,500
Total Estimated Cost		$121,100

D. Risk Assessment

Several risks are inherent in the design and development phase of Sandia Valley Bank's GRC maturity project; therefore, it is necessary to assess those risks so that the project's development and deployment are successful. The first major risk is that the GRC platform is incorrectly configured. This incorrect configuration increases the likelihood of obtaining inaccurate data about risks, which would make the reports unreliable. Second, there is a

moderate chance of misconfiguration, given the presence of basic access control; however, the resulting disruption to compliance processes will be moderate. Third, the lack of complete or up-to-date documentation regarding policies is likely to arise as a direct result of the time constraints present in the development process. Although documented templates for policies are available, failure to update them may lead to audit deficiencies, thereby creating a less favorable position for the bank regulators. Fourth, there is a high-priority risk related to unauthorized access to the risk register database, which contains sensitive operational and security data. Since the risk register data is stored in an encrypted manner and users must use multi-factor authentication before gaining access to the database, the high likelihood of a possible breach positions this risk at the top of the priority list. In addition to these four major risks, the bank also faces the possibility of failing to adequately evaluate its vendors due to gaps in its current vendor management process. This failure could expose SVB to supply chain vulnerabilities that could negatively impact service availability or compromise customer data protection. Another high-priority risk the bank faces is timeline delays, as other IT projects within the organization may compete for the same personnel resources, limiting the availability of qualified employees to work on this project and thereby increasing the time required to reach key project milestones. Finally, the bank is at risk due to the inability of employees working on the GRC development project to dedicate sufficient time to their assigned duties, resulting from excessive internal workload requirements. This could compromise the quality of the documentation created or slow down the overall project progress.

Both the quantitative and qualitative factors show that most of the risks mentioned would have a moderate to high operational impact. Misconfigured GRC tools may require an

additional 30–40 hours of effort to correct, incomplete policies could lead to costly audit remediation efforts, unauthorized access to the database could incur high financial costs to investigate and contain the damage, missing vendor evaluations could lead to expensive downtime, and timeline delays may increase project costs. All these risks demonstrate that the costs and benefits associated with each one favor mitigation, where the cost of mitigation is relatively low in comparison to the potential negative impact on the organization should the risks remain unresolved.

The primary objective of the various mitigation strategies identified is to enhance controls and improve project governance. To minimize the risks of GRC tool misconfiguration, the project will conduct regular formal testing cycles, include the vendors in the testing cycles, and allow cross-departmental review of all testing results. To mitigate the risks of incomplete or out-of-date policy documentation, the project will assign policy owners who are clearly identifiable, develop and utilize structured approval workflow models, and utilize standardized policy template documents. To mitigate unauthorized access to the risk register database, the project will use strict least privilege controls, monitor system usage more frequently, and require mandatory multi-factor authentication for all users. To mitigate vendor evaluation risks, the project will implement a tiered vendor model, establish and enforce standardized due diligence procedures, and conduct annual reviews of all vendors to ensure ongoing compliance. To mitigate timeline delays, the project will plan and report milestones on a weekly basis and make resource reallocations based upon these outcomes. By combining these mitigation strategies, SVB will be able to effectively minimize operational and compliance risks while ensuring the success of the GRC maturity project.

E. Justification

This proposed GRC maturity solution will better address SVB's business issue than other available options due to its ability to centralize, standardize, and structure the bank's management of cybersecurity, compliance, and operational risk management. SVB is facing several problems that contribute to its inability to effectively manage and protect the bank from cyberattacks and regulatory audits. These include:

- A lack of a cohesive policy, with multiple departments creating separate and potentially conflicting policies.
- Multiple, inconsistent risk assessments are being performed across different departments and locations within the bank.
- There is currently very little visibility into the threats facing the bank, either internally or externally.
- Vendor oversight is limited.

Therefore, the bank requires a single solution that can integrate risk information from disparate systems, automate compliance-related activities, and support evidence-based decision-making. The solution should be able to utilize the NIST Cybersecurity Framework, as well as the FFIEC guidelines and the GLBA Safeguards Rules, to ensure compliance with bank regulations. This will allow SVB to establish a consistent process for achieving long-term security and compliance.

Alternative approaches to developing a GRC solution included enhancing the bank's use of spreadsheets and manual processes, as well as implementing a point solution such as a standalone risk-scoring tool. However, neither alternative can scale to meet the increasing

demands placed upon SVB by its expanding digital footprint, nor can it meet the need for automated processes or cross-functional departmental collaboration. The use of manual processes increases the potential for human errors, results in inconsistent auditing, and does not provide timely visibility into the threats facing the bank. Furthermore, using point solutions creates duplicate effort and inaccurate reporting. In contrast to these alternatives, a comprehensive, single-system GRC program can provide policy management, risk tracking, vendor oversight, and compliance monitoring.

A comprehensive GRC program enables better governance, facilitates more effective control implementations, and supports better resource utilization, thereby addressing both the immediate business needs of SVB and positioning them for future regulatory changes, operational expansion, and emerging cybersecurity threats.

F. Resource Management Plan

The execution of the GRC maturity project at SVB will depend on an integrated approach to managing available resources, ensuring that this GRC project continues to progress efficiently alongside other IT and compliance projects that are also being worked on. Primary resources that are necessary for the project design and delivery include: A GRC software platform, trained IT and cybersecurity personnel, compliance and audit personnel, project management tools, vendor-provided training, and secure workstations for analysis and documentation. Each of the resources listed is necessary because the GRC project relies on accurate risk data, updated policy documents, and effective governance processes that require collaboration across departments, technical expertise, and reliable technology infrastructure.

These resources are all critical to the achievement of the project's goals. The justification for selecting a GRC platform is to enable centralized risk assessments, automated compliance workflows, and consistent reporting capabilities for the bank. The IT and cybersecurity personnel will be used to configure controls, perform system integrations, and validate risk and policy data. The compliance and audit personnel will be responsible for ensuring alignment with regulatory standards and providing subject matter input related to GLBA, FFIEC, and internal audit requirements. Project management tools will be used to track timelines, manage dependencies, and monitor progress on the project, since there are many high-priority projects running concurrently. Vendor-led GRC training will be necessary to ensure that staff can correctly interpret the data, manage risk processes, and operate the new system efficiently. Secure workstations and documentation resources will be necessary to support accurate analysis and protect sensitive regulatory and risk information.

Resources will be allocated using a phased approach that prioritizes the work according to risk, regulatory deadlines, and workforce availability. In the early stages of the project, resource allocation will focus on compliance staff, security analysts, and project managers to establish governance structures, develop policies, and build the initial risk register. During the development phase of the project, technical resources will be allocated to system configuration, control mapping, and vendor integration. Responsibilities will be distributed across departments with clear task assignments based upon expertise and capacity to avoid overburdening staff. Weekly coordination meetings and workload reviews will provide the ability to shift resources when needed and to prevent excessive disruption to staff working on other IT projects.

Several existing gaps within the organization make these resources critical to supporting the needs of the GRC project. The bank currently lacks a centralized repository for policy documents, risk data, and vendor assessments, which leads to inefficient processes and duplicated efforts between departments. By filling these gaps, the organization will experience improved risk visibility and a better regulatory posture; however, there may be some temporary redirection of personnel away from active projects such as infrastructure upgrades, cloud migration, or software rollouts. In the long term, the organization will benefit from having fewer audit findings, reduced manual work, clearer documentation standards, and improved coordination across the concurrency of initiatives. The resource management plan provides assurance that the GRC project continues to move forward in an efficient manner while maintaining stability in the bank's broader project portfolio.

G. Overall Project Plan

Scope:

This project is about creating a complete GRC maturity program for SVB, which includes designing and developing the unified governance structure, updating and centralizing security policies, developing an enterprise risk register, implementing a GRC platform, improving vendor risk management processes, and developing multi-year roadmap for maturity that is aligned with NIST CSF, FFIEC guidance, and GLBA requirements.

Assumptions:

The assumption for this project is that all the primary stakeholders (IT staff, cybersecurity analysts, compliance officers, and internal audit personnel) are available to collaborate during

the various phases of the project. It is also assumed that SVB will obtain approval and purchase the necessary GRC software licenses prior to the start of the development phase, ensuring no delay in configuring the platform. This project also assumes that all the internal data sources, such as existing policies, risk assessments, vendor documentation, and audit reports, are readily available and have sufficient accuracy to support the design and build of the risk register and governance framework updates. Additionally, it is assumed that executive leadership will continue to support the project, remove any obstacles, and authorize resource allocation as necessary. Lastly, this project assumes that there will be no major organization-wide disruptions, such as significant regulatory issues or system outages, which could divert resources away from the project and disrupt the timeline.

Project Phases:

1. Planning and requirements gathering
2. Design the governance structures, risk frameworks, and standard operating policies
3. Develop the risk register, vendor risk process, and configure the GRC platform
4. Test and validate
5. Implement and train employees
6. Review post-implementation and lessons learned

Timeline:

- Phase 1: Planning and requirements gathering
    a. December 4, 2025 – December 20, 2025
- Phase 2: Governance structures, risk frameworks, and standard operating procedures
    a. January 5, 2026 – January 31, 2026

- Phase 3: Develop the risk register, vendor risk process, and configure the GRC platform
    a. February 1, 2026 – March 20, 2026
- Phase 4: Test and validate
    a. March 21, 2026 – April 10, 2026
- Phase 5: Implement and train employees
    a. April 11, 2026 – May 5, 2026
- Phase 6: Review post-implementation and lessons learned
    a. May 6, 2026 – May 20, 2026

Dependencies:

- The GRC software license is acquired in a timely manner
- There are Subject Matter Experts (SME's) in compliance, audit, and security
- Data from existing systems and vendor files are accurate
- Scheduled IT maintenance windows for system integration
- The project manager and staff have been assigned their roles

Risk Factors:

- Resource strain from other active IT projects
- Delays in acquiring a license or onboarding a vendor
- Incomplete policy or risk data that needs additional revisions
- Challenges in configuring the GRC platform
- The employees are resistant to change with the unfamiliar workflows

Important Milestones:

- Completion of all required documents – March 31, 2026
- Finalized GRC framework and standard operating policy drafts – April 30, 2026
- Fully built risk register – June 5, 2026
- GRC platform configuration is complete – June 20, 2026
- Testing approval and sign off – July 10, 2026
- Go live launch – July 25, 2026
- Final project review and lessons learned – August 20, 2026

Project Launch Details:

The project will begin with a formal “kick-off” meeting, attended by senior IT leadership, cybersecurity, compliance, vendor management, and executive-level stakeholders. This meeting will cover the project scope, timelines, roles and responsibilities, communications, and expectations. By doing this at the start, we will have a clear understanding of what is expected of us and ensure that everyone is aligned before beginning the design phase.

Implementation Strategy:

The implementation plan is a phased/risk-based plan. The team will complete high-impact items, such as the risk register, governance model, and updated policies, first. Then, they will configure the GRC platform in accordance with those items to ensure accuracy and consistency. Our testing will be focused on validating the workflow, permissions, reporting, and vendor assessments, as well as conducting training sessions for all users. To minimize disruptions, the project team will test the solution before full deployment to ensure it is working properly and to minimize daily bank operations.

Documentation Deliverables:

- Governance framework documentation
- Updated policy suite
- Enterprise risk register
- GRC platform configuration guide
- Vendor risk management procedures
- Multi-year maturity roadmap
- Training materials and user guides for employees
- Final project summary and executive report

Hardware and Software Deliverables:

- New secure workstations for GRC analysts
- Licensed GRC platform
- Secure storage for risk and compliance data
- Access control configurations and multi-factor authentication
- Backup and archive tools for risk and policy data

Evaluation Framework for Final Output:

The final solution will be assessed against established industry and regulatory criteria. The level of maturity in managing risks, as measured against the NIST cybersecurity framework, will assess how well the organization aligns with the framework for measuring its risk management process. Inherent risk, control maturity, and governance effectiveness will be measured using the FFIEC Cybersecurity Assessment Tool's domain structure. Compliance with the GLBA Safeguards Rule requirements will be used to determine if adequate administrative,

technical, and physical security controls have been implemented as required. Standards for internal auditing, along with documented control mappings, will be used to assess the completeness, reliability, and accuracy of the GRC processes. Success will be evident by higher maturity scores, fewer control gaps, and increased readiness for audits.

References

Cybersecurity Assessment Tool | FFIEC. (2025, March 29). Ffiec.gov. https://www.ffiec.gov/resources/cat

FTC safeguards rule: What your business needs to know. (2024, December 23). Federal Trade Commission. https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know

National Institute of Standards and Technology. (2018). Framework for improving Critical Infrastructure Cybersecurity. In *National Institute of Standards and Technology*. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

PCI Security Standards Council. (2024, July 12). *PCI Security Standards Council – Protect Payment Data with Industry-driven Security Standards, Training, and Programs*. https://www.pcisecuritystandards.org/standards/